PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140244

(43)Date of publication of application : 17.05.2002

---

(51)Int.Cl. G06F 13/00

G06F 15/00

H04L 9/32

---

(21)Application number : 2000-332093 (71)Applicant : MCM JAPAN KK

(22)Date of filing : 31.10.2000 (72)Inventor : SANETO TORU

---

(54) METHOD FOR PROVIDING NETWORK SERVICE, AND DEVICE UTILIZING THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To realize an arrangement enabling a user to easily receive a network service.

SOLUTION: A network terminal 18 for receiving the provision of a network service is connected to the Internet 12. The user receives the provision of the network service using the network terminal 18. A service key 20 is connected to the network terminal 18. The user can receive the provision of the network service only by attaching the service key 20 to the network terminal 18, since various information or software for receiving the network service is stored in the service key 20. Consequently, it is not necessary to make various conventional settings to the network terminal 18 beforehand, and the user can easily receive the provision of the network service.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It is the storage characterized by including service application software for said information receiving a predetermined network service through a network in the storage which stored the information for network connection.

[Claim 2] It is the storage characterized by including the application ID which specifies the service which is ID which can attest the authentication server of said exterior with the data for personal authentication for said information to perform a user's personal authentication further in a storage according to claim 1, and the network setting data for carrying out network connection to an external authentication server, and is offered.

[Claim 3] It is the storage characterized by said information containing the number of said user's credit card further in a storage according to claim 1.

[Claim 4] The network terminal equipped with an R/W means to write data to a storage according to claim 1 to 3, and a network connection means to connect with a predetermined network.

[Claim 5] Router equipment equipped with an R/W means to write data to a storage according to claim 1 to 3, and a network connection means to connect with a predetermined network.

[Claim 6] Server equipment equipped with an R/W means to write data to a storage according to claim 1 to 3, and a network connection means to connect with a predetermined network.

[Claim 7] The service key characterized by including the network interface for connecting with a storage according to claim 1 to 3 and external electronic equipment.

[Claim 8] The service key characterized by including the network interface for connecting with a storage according to claim 1 to 3 and external electronic equipment, and the luminescence means by which a lighting condition is controlled from the electronic equipment of said exterior.

[Claim 9] It is the service key characterized by said network interface being a USB interface in a service key according to claim 7 or 8.

[Claim 10] The network terminal equipped with the connecting means for connecting with said network interface of a service key according to claim 7 or 8, and a network connection means to connect with a predetermined network.

[Claim 11] Router equipment equipped with the connecting means for connecting with said network interface of a service key according to claim 7 or 8, and a network connection means to connect with a predetermined network.

[Claim 12] Server equipment equipped with the connecting means for connecting with said network interface of a service key according to claim 7 or 8,

and a network connection means to connect with a predetermined network.

[Claim 13] The network service offer approach characterized by including the step which connects to a network terminal the storage which stored the service application software for receiving a predetermined network service through a network, the starting step which said service application software starts on said network terminal, and the service provision step from which a user receives offer of predetermined service using said service application software which started.

[Claim 14] In the network service offer approach according to claim 13 said storage Furthermore, data for personal authentication for performing said user's personal authentication and network setting data for carrying out network connection to an external authentication server, The application ID which specifies the service which is ID which can attest the authentication server of said exterior, and is offered The authentication data input step into which it stores in and said user inputs authentication data using said service application software, When both are in agreement with the comparison collating step which carries out comparison collating with said data for personal authentication in said storage as a result of said collating, said inputted authentication data The accounting step which starts accounting by offer of the service which carries out network connection to the authentication server of said exterior using said network setting data, and is specified by said application ID, When both are not

in agreement as a result of said collating The network service offer approach which carries out network connection to the authentication server of said exterior using said network setting data, and is characterized by including the deletion step which deletes the data about accounting of the service specified by said application ID.

[Claim 15] The network service offer approach characterized by including the removal step to which said user removes said storage from said network terminal, and the application deletion step from which said service application within said network terminal is deleted after said storage is removed in the network service offer approach according to claim 13.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to offer of the network service using the service key which memorized predetermined network connection information.

[0002]

[Description of the Prior Art] In recent years, various services are offered through

the network represented by the Internet.

[0003]

[Problem(s) to be Solved by the Invention] However, in order to receive offer of service through the Internet, a user has to perform a setup for receiving the service in the terminal connected to the Internet. Moreover, it is necessary to install the special individual application for receiving service in a terminal beforehand.

[0004] Consequently, the complicated activity was required in order to receive offer of various services through the Internet.

[0005] This invention is made in view of such a technical problem, and the purpose is realizing the structure from which a user's can receive a network service easily.

[0006]

[Means for Solving the Problem] In order that this invention may solve the above-mentioned technical problem, in the storage which stored the information for network connection, said information is a storage characterized by including the service application software for receiving a predetermined network service through a network.

[0007] If this storage is used, the software for receiving a network service is acquirable with such a configuration.

[0008] Moreover, said information is ID which can attest the authentication server of said exterior with the data for personal authentication for performing a user's personal authentication, and the network setting data for carrying out network connection to an external authentication server further, and this invention is a storage characterized by including the application ID which specifies the service to offer.

[0009] Information required for network connection is acquirable with such a configuration.

[0010] Moreover, this invention is a storage characterized by said information containing the number of said user's credit card further.

[0011] The above-mentioned credit card number can be used for accounting to network connection by such configuration.

[0012] Moreover, this invention is the network terminal equipped with an R/W means to write data to said storage, and a network connection means to connect with a predetermined network.

[0013] Moreover, this invention is router equipment equipped with an R/W means to write data to said storage, and a network connection means to connect with a predetermined network.

[0014] Moreover, this invention is server equipment equipped with an R/W means to write data to said storage, and a network connection means to connect

with a predetermined network.

[0015] It is possible to receive a network service by configuration like these network terminals, router equipment, and server equipment using the information in said storage.

[0016] Moreover, this invention is a service key characterized by including the network interface for connecting with a storage and external electronic equipment.

[0017] According to such a configuration, external electronic equipment and connection are easy, and can receive a network service easily.

[0018] Moreover, this invention is a service key characterized by including the network interface for connecting with a storage and external electronic equipment, and the luminescence means by which a lighting condition is controlled from the electronic equipment of said exterior.

[0019] A luminescence means is controllable by such configuration from external electronic equipment.

[0020] Moreover, this invention is a service key characterized by said network interface being a USB interface.

[0021] According to such a configuration, a service key is easily connectable with external electronic equipment with a USB interface.

[0022] Moreover, this invention is the network terminal equipped with the

connecting means for connecting with said network interface of the above-mentioned service key, and a network connection means to connect with a predetermined network.

[0023] Moreover, this invention is router equipment equipped with the connecting means for connecting with said network interface of the above-mentioned service key, and a network connection means to connect with a predetermined network.

[0024] Moreover, this invention is server equipment equipped with the connecting means for connecting with said network interface of the above-mentioned service key, and a network connection means to connect with a predetermined network.

[0025] It is possible to receive a network service by configuration like these network terminals, router equipment, and server equipment using the information in said service key.

[0026] Moreover, this invention is the network service offer approach characterized by including the step which connects to a network terminal the storage which stored the service application software for receiving a predetermined network service through a network, the starting step which said service application software starts on said network terminal, and the service provision step from which a user receives offer of predetermined service using

said service application software which started.

[0027] By such configuration, a user can receive a network service easily using the software in a storage.

[0028] Moreover, the data for personal authentication for said storage to perform said user's personal authentication further in this invention, The network setting data for carrying out network connection to an external authentication server, The application ID which specifies the service which is ID which can attest the authentication server of said exterior, and is offered The authentication data input step into which it stores in and said user inputs authentication data using said service application software, When both are in agreement with the comparison collating step which carries out comparison collating with said data for personal authentication in said storage as a result of said collating, said inputted authentication data The accounting step which starts accounting by offer of the service which carries out network connection to the authentication server of said exterior using said network setting data, and is specified by said application ID, When both are not in agreement as a result of said collating It is the network service offer approach which carries out network connection to the authentication server of said exterior using said network setting data, and is characterized by including the deletion step which deletes the data about accounting of the service specified by said application ID.

[0029] such a configuration -- him, a user, -- since collating is performed using the information in a storage -- simple -- him -- it is possible to perform collating.

[0030] Moreover, this invention is the network service offer approach characterized by including the removal step to which said user removes said storage from said network terminal, and the application deletion step from which said service application within said network terminal is deleted after said storage is removed.

[0031] After a storage is removed by such configuration, it is possible to delete automatically the software which was being used for the network service.

[0032]

[Embodiment of the Invention] Hereafter, the gestalt of suitable operation of this invention is explained based on a drawing.

[0033] Gestalt 1 drawing 1 of operation is the block diagram of the network system 10 with which offer of the network service of the gestalt 1 of this operation is carried out.

[0034] As shown in this drawing, the network system 10 is equipped with the Internet 12, authentication/accounting server 14 linked to this Internet 12, and the service server group 16 linked to the Internet 12.

[0035] The network terminal 18 which receives offer of a network service is connected to the Internet 12. A user receives offer of a network service using

this network terminal 18.

[0036] It being characteristic in the gestalt of this operation is that the service key 20 is connected to the network terminal 18. The various information and software for receiving a network service are stored in this service key 20, and a user only attaches this service key 20 in the network terminal 18, and can receive offer of a network service. The service key 20 is a key which uses as main components the storage with which predetermined information was stored. About details, such as information stored, it mentions later.

[0037] Consequently, it is not necessary to use as the network terminal 18 beforehand various setup mentioned above, and a user can receive offer of a network service easily.

[0038] Hereafter, the flow of actuation of offer of the network service in the gestalt 1 of this operation is explained to a detail.

[0039] A. Initial user registration **** and the user who wants to receive offer of predetermined service register into service key 20 grade the information about the service which he wants to receive. The flow chart showing this actuation is shown in drawing 2 .

[0040] In step S2-1 of this drawing, a user attaches the service key 20 in the network terminal 18. As long as the service key 20 is the storage which can memorize information, what kind of thing is sufficient as it. Although storages,

such as a floppy (trademark) disk and CD-R, may be used, the USB (Universal Serial Bus) plug which built in the flash memory, for example is desirable. Especially by the following explanation, unless it refuses, the example which constituted the service key 20 from this USB plug is explained. Even if the various devices by the specification of USB do not drop the power source of the network terminal 12, since installation and removal are possible, they can perform quickly installation and removal of the service key 20. Moreover, since the drive equipment which drives CD-R etc. is also unnecessary, not only the service key 20 but the network terminal 18 can be constituted small.

[0041] Next, in step S2-2, the network terminal 18 detects that the service key 20 was attached in the network terminal 18 (it connected). The structure which detects the connection condition automatically [as mentioned above, even if the device connected by USB specification does not drop a power source, connection and separation are possible for it, and / whenever it is connection] is well known from the former.

[0042] Step S In 2-3, the device driver of the USB device is read from the detected service key 20. And this device driver starts on the network terminal 18.

[0043] Step S In 2-4, an initialization authentication data write-in program is read from the service key 20. And this initialization authentication data write-in program starts on the network terminal 18. This program is a program for storing

the data specified by a user in the service key 20 interior. By using this program, a user can store predetermined data in the service key 20 interior freely.

[0044] Step S In 2-5, a user inputs authentication data according to directions of an initialization authentication data write-in program. Similarly, a user also inputs a credit card number. Similarly, a credit card password is also entered.

[0045] In addition, authentication data are data showing the user being him, and various data are used. Generally fingerprint data, the data of a password, etc. are used as authentication data.

[0046] Moreover, three sorts of data, "authentication data", a "credit card number", and a "credit card password", are named "personal data" generically in the text.

[0047] Step S In 2-6, the these-inputted data are written in the service key 20 interior by the initialization authentication data write-in program. The service newly registered into coincidence is registered into the database of the service key 20 interior. By forming such a database in the service key 20 interior, it can know whether such service is permitted to the user.

[0048] Step S In 2-7, the these-inputted data are notified to authentication/accounting server 14 by the initialization authentication data write-in program.

[0049] Step S In 2-8, authentication / accounting server 14 registers into the

authentication / accounting server 14 interior the various data by which the notice has been given [above-mentioned].

[0050] Step S In 2-9, check lamp 20c (refer to drawing 6) prepared in the service key 20 lights up. This lighting is performed by the initialization authentication data write-in program. A user can know that initial user registration was completed by lighting of this check lamp 20c. Moreover, initial user registration is completed and lighting of this check lamp 20c also means that the service key 20 may be removed from the network terminal 18.

[0051] B. A user actually explains the actuation which receives offer of service using the service key 20 based on the flow chart of drawing 3 below systems operation actuation.

[0052] In step S3-1, a user attaches the service key 20 in the network terminal 18 first.

[0053] Next, in step S3-2, the network terminal 18 detects that the service key 20 was attached in the network terminal 18 (it connected). This actuation is the same as that of the above-mentioned step S2-2.

[0054] Step S In 3-3, the device driver of the USB device which constitutes the service key 20 is read from the detected service key 20. And this device driver starts on the network terminal 18. This actuation is the same as that of the above-mentioned step S2-3.

[0055] Step S In 3-4, the database for service and service application are read from the service key 20. The database for service is stored in the network terminal 18 interior, and service application is started on the network terminal 18. Service application is software which operates on the network terminal 18, in order to provide a user with a predetermined network service. Especially this service application displays an application icon on the screen of the network terminal 18 after that starting. This application icon is an icon which makes a predetermined network service start, and if a user clicks on this icon, offer of a corresponding network service will be started.

[0056] Now, as for the above-mentioned database for service, and the above-mentioned service application, it is also desirable to compress and to store in the service key 20 interior. It compresses, and to store, before starting on storing or the network terminal 18 on the network terminal 18, it is necessary to once thaw. Here, compression means performing compression coding and means especially lossless compression.

[0057] Moreover, the database for service is a database with which the network service which a user can use is described.

[0058] Moreover, it is also desirable in this case to read the middleware which service application uses from the service key 20, and to use it. If middleware is used, it is possible to make service application and other software cooperate.

[0059] Step S In 3-5, a user inputs authentication data to the network terminal 18.

[0060] Step S In 3-6, the authentication data which the user inputted, and the authentication data already stored in the service key 20 interior are collated. Consequently, when both are not in agreement, it shifts to step S4 -1 of drawing 4 , and in being in agreement, processing shifts to step S4 -2 of drawing 4 . In addition, semantics differs from "coincidence" here according to the class of authentication data. In the case of a password, this "coincidence" means "full coincidence", but it says carrying out "both data approximating, so that it accepts as the authentication data by the same people" of the case of fingerprint data.

[0061] In step S4 -1, the purport were not in agreement is transmitted to authentication / accounting server 14. And authentication / accounting server 14 deletes the authentication account data stored in the interior.

[0062] In step S4 -2, the network terminal 18 eliminates the "personal data" stored in the interior of the service key 20 following on above-mentioned step S4 -1. And offer of a network service is stopped. A user has to perform "initial user registration" again mentioned above to receive a network service.

[0063] In step S4 -3, in order that a user may receive a certain predetermined network service, it clicks on the application icon of the network service.

[0064] In step S4 -4, service application notifies initiation of service to authentication/accounting server 14 according to the click of the

above-mentioned icon. This service is various network services known conventionally. For example, they are the animation distribution service on the Internet (television broadcasting), a connection service to distribution of music data and various databases, etc.

[0065] In addition, it is desirable to perform the notice using the identifier called Application ID in the case of a notice. This application ID is the identifier of the service to offer. This application ID is explained later.

[0066] In step S4 -5, authentication/accounting server 14 starts accounting according to the notice in above-mentioned step S4 -4. Furthermore, authentication/accounting server 14 notifies that accounting was started to the service server (group) 16.

[0067] In step S4 -6, the service server 16 starts predetermined service according to the notice in above-mentioned step S4 -5.

[0068] In step S4 -7, when service application accesses the service server 16, a user is provided with service.

[0069] Next, in step S5-1 of drawing 5 , in order to suspend service, a user closes the above-mentioned service icon. Then, in step S5-2, service application notifies having closed the service icon to authentication/accounting server 14.

[0070] Step S In 5-3, authentication/accounting server 14 stops accounting according to the notice in the above-mentioned step S5-2. Moreover, it notifies

that authentication/accounting server 14 stopped accounting to the service server 16.

[0071] Step S In 5-4, the service server 16 suspends service according to the notice in the above-mentioned step S5-3.

[0072] And in step S5-5, a user removes the service key 20 from the network terminal 18.

[0073] Step S In 5-6, all the data (software is included) developed from the service key 20 are deleted from the network terminal 18 according to the service key 20 having been removed. Although anyone may perform this deletion, the device driver of the service key 20 is deleting with the gestalt of this operation. With the gestalt of this operation, since the service key 20 uses the USB plug which built in the flash memory, the above-mentioned device driver is a device driver of USB.

[0074] If it is a location with the network terminal 18, without carrying out a complicated setup by attaching the service key 20 in the network terminal 18 according to the gestalt 1 of this operation as stated above, offer of a network service can be received anywhere.

[0075] With the gestalt 1 of the gestalt 2 (configuration of service key) above-mentioned implementation of operation, the service key 20 used the USB plug which built in the flash memory. The block diagram of such a service key 20

is shown in drawing 6 .

[0076] As shown in this drawing, the service key 20 contains flash memory 20b in body 20a of a USB plug. As mentioned above, various data and software are stored in this flash memory 20b. It will be as follows if those data and software are enumerated.

[0077] (1) Device driver : since the service key 20 uses the USB plug with the gestalt of this operation, this device driver is a USB driver. In adopting another gestalt as a service key 20, it adopts the device driver of other classes.

[0078] (2) Middleware : it is the software for operating the following service application.

[0079] (3) Service application : it is the software which offers a network service. Fundamentally, only the number of the service to offer is required for this service application. Of course, you may make it correspond to two or more services with one service application.

[0080] (4) (individual) -- authentication data: -- they are fingerprint data, a password, etc. This data is stored in case initial user registration is performed.

[0081] (5) Network setting data to authentication/accounting server 14 : this data is setting data required in order to charge by having authentication/accounting server 14 performing authentication, and is data with which the credit card number mentioned above is contained. This data is also written in in the service

key 20 in the above-mentioned initial user registration.

[0082] (6) Application ID which can recognize authentication/accounting server 14 : this ID is ID for a user to identify authentication/accounting of as opposed to which service for two or more services should be performed, when available. That is, it is the identifier of service.

[0083] (7) The credit card number for accounting : this data is the number of the credit card for accounting. Authentication/accounting server 14 is charged using this credit card number.

[0084] (8) Database : the service accepted to the user of this service key 20 is registered into this database. This database is updated in the above-mentioned initial user registration. It is possible by forming such a database especially to store two or more service applications in the service key 20 interior beforehand. The information on the service permitted to the user is registered into the database, and it constitutes so that service application may start only about the service registered. Consequently, providing the user with the service which is not registered into a database, i.e., the service which is not permitted to the user, accidentally is lost.

[0085] As for these data and a software group, it is desirable to compress (compression coding) and to store in flash memory 20b of the service key 20 suitably. Moreover, as for the data sent outside through a network, for example,

the data of above-mentioned (4) - (7) sent to authentication/accounting server 14, it is desirable to encipher in order to prevent to be diverted to others.

[0086] Moreover, as shown in drawing 6 , check lamp 20c equivalent to the luminescence means of this invention is prepared in the service key 20. This check lamp 20c consists of light emitting diodes etc., and that lighting condition is controlled from the external network terminal 18. Actuation of check lamp 20c was already explained in the top.

[0087] Moreover, as shown in drawing 6 , 20d of USB plug sections is prepared in the service key 20. 20d of this USB plug section carries out checking and verifying to the USB interface prepared in the network terminal 18, and it is connected electrically.

[0088] Of course, the gestalten 1 and 2 of this operation are available with mere storages, such as CD-R, a floppy disk, etc. by which the above information is stored, although the configuration equipped with the USB interface which is a network interface as a service key 20 was adopted. In the case of such a storage, it is necessary to have drive equipment (for it to be able to set to this invention) "an R/W means" with which the network terminal 18 can perform R/W of data to those storages.

[0089] The gestalt 3 (configuration of network terminal) network terminal 18 of operation can use the various electronic equipment which can connect with a

network. Typically, the so-called personal computer can be used as a network terminal 18. Furthermore, it is also desirable to use as a network terminal 18 in the gestalt of this operation of the router and server linked to a network.

[0090] These network terminals 18 needed to connect the service key 20, and need to be equipped with the means in which reading and **** of the data of the interior or software are possible.

[0091] For example, in order to use the service key 20 of the USB plug mold shown by above-mentioned drawing 6 , the network terminal 18 needs to be equipped with the USB interface.

[0092] the gestalt 4 (use gestalt of a share and others of the service key by two or more users) of operation -- although it is a typical use gestalt that an individual carries his own service key 20, connects the service key 20 to the network terminal 18 which is in near if needed, and the service key 20 receives offer of a network service again, it is a desirable employment gestalt that two or more users also share one service key 20.

[0093] Furthermore, it is also desirable to store two or more service applications in the service key 20 interior, and if an initial user setup is performed for every service, it is possible to receive offer of two or more network services with one service key 20.

[0094] The thing [, preparing the separate service key 20 for every service on the

other hand] is also desirable. If one service is made to always correspond to one service key 20, management of the service key 20 will not become complicated, but management will become easy.

[0095] Moreover, extending also to an office application is possible.

[0096] Although the authentication accounting server 14 performs gestalt 5 (accounting) accounting of operation, this accounting can adopt various accounting systems. It is also desirable to charge based on the amount of data which could charge by the count of the service to offer and was transmitted by service. Furthermore, it is also desirable to charge by time amount while the service icon is opened.

[0097] The various services on a network can be received simply, without a user being conscious of a setup of a specific network by according to the gestalten 1-3 of this operation, an individual's holding the service key 20 and attaching in various kinds of network terminals, as stated above. Therefore, if even the service key 20 is held, it is possible to receive a predetermined network service from the location of arbitration in which the network terminal 18 is installed.

[0098] the gestalt 6 (in addition to this) of operation -- ********** [the number of them / what] in addition as long as the service server 16 is one or more pieces. Moreover, one service server 16 may offer two or more kinds of services. Moreover, each service may be offered respectively independently of a separate

service server.

[0099] As long as authentication/accounting server 14 is also one or more pieces, how many pieces are sufficient. A different authentication/accounting server 14 for every service may be used.

[0100]

[Effect of the Invention] As stated above, according to this invention, a user can receive a network service simple.

[0101] Moreover, if it is the location in which the network terminal (for example, a router and a server) by this invention is located, a user will become possible [receiving offer of a network service] anywhere.

[0102] Moreover, since it also has the interface which information required in order to receive a network service is stored, and can be connected to electronic equipment according to the service key of this invention, this service key is connected to various electronic equipment, and it enables a user to receive offer of a network service.

[0103] Moreover, according to this invention, since the service application in a storage starts, a user can receive offer of a network service simple. furthermore, the information in a storage -- being based -- him -- since it attests -- him -- authentication can be performed simple. And if a storage is removed from a network terminal, the software inside a network terminal will be deleted.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－140244
（P2002－140244A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	５１０	Ｇ０６Ｆ　13/00	５１０Ａ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｇ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	
			６７３Ｅ	

審査請求　未請求　請求項の数15　ＯＬ　（全　９　頁）

(21)出願番号　特願2000－332093(P2000－332093)

(22)出願日　平成12年10月31日(2000.10.31)

(71)出願人　595161887
エム・シー・エムジャパン株式会社
東京都世田谷区三軒茶屋２－11－22　サンタワーズセンタービル

(72)発明者　実藤　亨
東京都世田谷区三軒茶屋２丁目11番22号　サンタワーズセンタービル　エム・シー・エムジャパン株式会社内

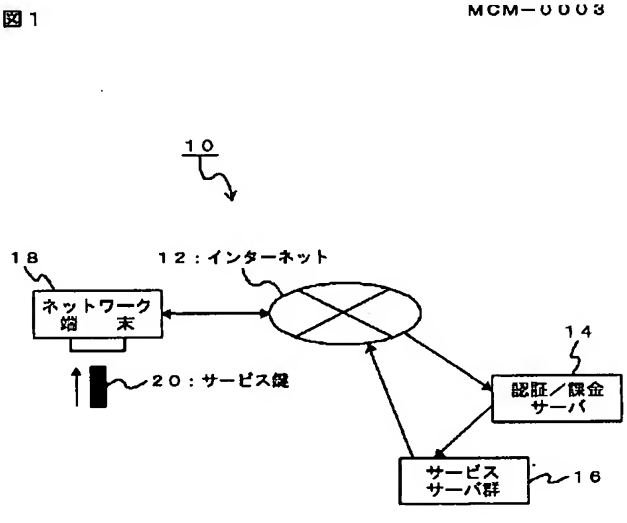
(74)代理人　100109014
弁理士　伊藤　充

Ｆターム(参考)　5B085 AC04 AE13 AE23
5J104 AA07 KA01 MA01 NA05 NA27
NA41 PA07 PA11

(54)【発明の名称】　ネットワークサービス提供方法及びそれに利用する装置

(57)【要約】
【課題】　利用者が簡単にネットワークサービスを受けることができる仕組みを実現することである。
【解決手段】　インターネット１２には、ネットワークサービスの提供を受けるネットワーク端末１８が接続されている。利用者はこのネットワーク端末１８を用いてネットワークサービスの提供を受ける。ネットワーク端末１８には、サービス鍵２０が接続される。このサービス鍵２０にはネットワークサービスを受けるための種々の情報やソフトウェアが格納されており、利用者はこのサービス鍵２０をネットワーク端末１８に取り付けるだけで、ネットワークサービスの提供を受けることができる。その結果、従来のように種々の設定をあらかじめネットワーク端末１８にしておく必要がなく、利用者は容易にネットワークサービスの提供を受けることができる。

図１



【特許請求の範囲】
【請求項１】　ネットワーク接続のための情報を格納した記憶媒体において、
前記情報は、
ネットワークを介して所定のネットワークサービスを受けるためのサービスアプリケーションソフトウェア、
を含むことを特徴とする記憶媒体。
【請求項２】　請求項１記載の記憶媒体において、
前記情報は、さらに、
利用者の個人認証を行うための個人認証用データと、
外部の認証サーバにネットワーク接続するためのネットワーク設定データと、
前記外部の認証サーバが認証可能なＩＤであって、提供するサービスを特定するアプリケーションＩＤと、
を含むことを特徴とする記憶媒体。
【請求項３】　請求項１記載の記憶媒体において、
前記情報は、さらに、
前記利用者のクレジットカードの番号、
を含むことを特徴とする記憶媒体。
【請求項４】　請求項１乃至３記載の記憶媒体に対してデータの読み書きを行う読み書き手段と、
所定のネットワークに接続するネットワーク接続手段と、を備えたネットワーク端末。
【請求項５】　請求項１乃至３記載の記憶媒体に対してデータの読み書きを行う読み書き手段と、
所定のネットワークに接続するネットワーク接続手段と、を備えたルータ装置。
【請求項６】　請求項１乃至３記載の記憶媒体に対してデータの読み書きを行う読み書き手段と、
所定のネットワークに接続するネットワーク接続手段と、を備えたサーバ装置。
【請求項７】　請求項１乃至３記載の記憶媒体と、
外部の電子機器と接続するためのネットワークインターフェースと、
を含むことを特徴とするサービス鍵。
【請求項８】　請求項１乃至３記載の記憶媒体と、
外部の電子機器と接続するためのネットワークインターフェースと、
前記外部の電子機器から点灯状態を制御される発光手段と、
を含むことを特徴とするサービス鍵。
【請求項９】　請求項７又は８記載のサービス鍵において、
前記ネットワークインターフェースは、ＵＳＢインターフェースであることを特徴とするサービス鍵。
【請求項１０】　請求項７又は８記載のサービス鍵の前記ネットワークインターフェースと接続するための接続手段と、
所定のネットワークに接続するネットワーク接続手段と、を備えたネットワーク端末。
【請求項１１】　請求項７又は８記載のサービス鍵の前記ネットワークインターフェースと接続するための接続手段と、
所定のネットワークに接続するネットワーク接続手段と、を備えたルータ装置。
【請求項１２】　請求項７又は８記載のサービス鍵の前記ネットワークインターフェースと接続するための接続手段と、
所定のネットワークに接続するネットワーク接続手段と、を備えたサーバ装置。
【請求項１３】　ネットワークを介して所定のネットワークサービスを受けるためのサービスアプリケーションソフトウェアを格納した記憶媒体をネットワーク端末に接続するステップと、
前記ネットワーク端末上で前記サービスアプリケーションソフトウェアが起動する起動ステップと、
前記起動したサービスアプリケーションソフトウェアを用いて利用者が所定のサービスの提供を受けるサービス提供ステップと、
を含むことを特徴とするネットワークサービス提供方法。
【請求項１４】　請求項１３記載のネットワークサービス提供方法において、
前記記憶媒体は、さらに、前記利用者の個人認証を行うための個人認証用データと、外部の認証サーバにネットワーク接続するためのネットワーク設定データと、前記外部の認証サーバが認証可能なＩＤであって、提供するサービスを特定するアプリケーションＩＤと、を格納しており、
前記利用者が、前記サービスアプリケーションソフトウェアを用いて、認証データを入力する認証データ入力ステップと、
前記入力された認証データを、前記記憶媒体内の前記個人認証用データと比較照合する比較照合ステップと、
前記照合の結果、両者が一致した場合には、前記ネットワーク設定データを用いて前記外部の認証サーバにネットワーク接続し、前記アプリケーションＩＤによって特定されるサービスの提供による課金を開始する課金ステップと、
前記照合の結果、両者が一致しない場合には、前記ネットワーク設定データを用いて前記外部の認証サーバにネットワーク接続し、前記アプリケーションＩＤによって特定されるサービスの課金に関するデータを削除する削除ステップと、
を含むことを特徴とするネットワークサービス提供方法。
【請求項１５】　請求項１３記載のネットワークサービス提供方法において、
前記利用者が前記記憶媒体を前記ネットワーク端末から取り外す取り外しステップと、

前記記憶媒体が取り外された後、前記ネットワーク端末内の前記サービスアプリケーションが削除されるアプリケーション削除ステップと、
を含むことを特徴とするネットワークサービス提供方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、所定のネットワーク接続情報を記憶したサービス鍵を利用したネットワークサービスの提供に関する。
【０００２】
【従来の技術】近年、インターネットに代表されるネットワークを介して種々のサービスが提供されている。
【０００３】
【発明が解決しようとする課題】しかし、インターネットを介してサービスの提供を受けるためには、ユーザはインターネットに接続された端末にそのサービスを受けるための設定を行わなければならない。また、サービスを受けるための特別な個別アプリケーションをあらかじめ端末にインストールしておく必要がある。
【０００４】その結果、インターネットを介して種々のサービスの提供を受けるためには、繁雑な作業が必要であった。
【０００５】本発明はこのような課題に鑑みなされたものであり、その目的は、利用者が簡単にネットワークサービスを受けることができる仕組みを実現することである。
【０００６】
【課題を解決するための手段】本発明は、上記課題を解決するために、ネットワーク接続のための情報を格納した記憶媒体において、前記情報は、ネットワークを介して所定のネットワークサービスを受けるためのサービスアプリケーションソフトウェア、を含むことを特徴とする記憶媒体である。
【０００７】このような構成によって、この記憶媒体を用いればネットワークサービスを受けるためのソフトウェアを取得することができる。
【０００８】また、本発明は、前記情報は、さらに、利用者の個人認証を行うための個人認証用データと、外部の認証サーバにネットワーク接続するためのネットワーク設定データと、前記外部の認証サーバが認証可能なＩＤであって、提供するサービスを特定するアプリケーションＩＤと、を含むことを特徴とする記憶媒体である。
【０００９】このような構成によって、ネットワーク接続のために必要な情報を取得することができる。
【００１０】また、本発明は、前記情報は、さらに、前記利用者のクレジットカードの番号、を含むことを特徴とする記憶媒体である。
【００１１】このような構成によって、上記クレジットカード番号を、ネットワーク接続に対する課金に利用することができる。
【００１２】また、本発明は、前記記憶媒体に対してデータの読み書きを行う読み書き手段と、所定のネットワークに接続するネットワーク接続手段と、を備えたネットワーク端末である。
【００１３】また、本発明は、前記記憶媒体に対してデータの読み書きを行う読み書き手段と、所定のネットワークに接続するネットワーク接続手段と、を備えたルータ装置である。
【００１４】また、本発明は、前記記憶媒体に対してデータの読み書きを行う読み書き手段と、所定のネットワークに接続するネットワーク接続手段と、を備えたサーバ装置である。
【００１５】これらのネットワーク端末、ルータ装置、サーバ装置のような構成によって、前記記憶媒体中の情報を利用してネットワークサービスを受けることが可能である。
【００１６】また、本発明は、記憶媒体と、外部の電子機器と接続するためのネットワークインターフェースと、を含むことを特徴とするサービス鍵である。
【００１７】このような構成によれば、外部の電子機器と接続が容易で、かつ、ネットワークサービスを簡単に受けることができる。
【００１８】また、本発明は、記憶媒体と、外部の電子機器と接続するためのネットワークインターフェースと、前記外部の電子機器から点灯状態を制御される発光手段と、を含むことを特徴とするサービス鍵である。
【００１９】このような構成によって、外部の電子機器から発光手段を制御することができる。
【００２０】また、本発明は、前記ネットワークインターフェースは、ＵＳＢインターフェースであることを特徴とするサービス鍵である。
【００２１】このような構成によれば、ＵＳＢインターフェースによって、容易にサービス鍵を外部の電子機器に接続することができる。
【００２２】また、本発明は、上記サービス鍵の前記ネットワークインターフェースと接続するための接続手段と、所定のネットワークに接続するネットワーク接続手段と、を備えたネットワーク端末である。
【００２３】また、本発明は、上記サービス鍵の前記ネットワークインターフェースと接続するための接続手段と、所定のネットワークに接続するネットワーク接続手段と、を備えたルータ装置である。
【００２４】また、本発明は、上記サービス鍵の前記ネットワークインターフェースと接続するための接続手段と、所定のネットワークに接続するネットワーク接続手段と、を備えたサーバ装置である。
【００２５】これらのネットワーク端末、ルータ装置、サーバ装置のような構成によって、前記サービス鍵中の情報を利用してネットワークサービスを受けることが可

能である。

【００２６】また、本発明は、ネットワークを介して所定のネットワークサービスを受けるためのサービスアプリケーションソフトウェアを格納した記憶媒体をネットワーク端末に接続するステップと、前記ネットワーク端末上で前記サービスアプリケーションソフトウェアが起動する起動ステップと、前記起動したサービスアプリケーションソフトウェアを用いて利用者が所定のサービスの提供を受けるサービス提供ステップと、を含むことを特徴とするネットワークサービス提供方法である。

【００２７】このような構成によって、記憶媒体中のソフトウェアを利用して、利用者は簡単にネットワークサービスを受けることができる。

【００２８】また、本発明は、前記記憶媒体は、さらに、前記利用者の個人認証を行うための個人認証用データと、外部の認証サーバにネットワーク接続するためのネットワーク設定データと、前記外部の認証サーバが認証可能なＩＤであって、提供するサービスを特定するアプリケーションＩＤと、を格納しており、前記利用者が、前記サービスアプリケーションソフトウェアを用いて、認証データを入力する認証データ入力ステップと、前記入力された認証データを、前記記憶媒体内の前記個人認証用データと比較照合する比較照合ステップと、前記照合の結果、両者が一致した場合には、前記ネットワーク設定データを用いて前記外部の認証サーバにネットワーク接続し、前記アプリケーションＩＤによって特定されるサービスの提供による課金を開始する課金ステップと、前記照合の結果、両者が一致しない場合には、前記ネットワーク設定データを用いて前記外部の認証サーバにネットワーク接続し、前記アプリケーションＩＤによって特定されるサービスの課金に関するデータを削除する削除ステップと、を含むことを特徴とするネットワークサービス提供方法である。

【００２９】このような構成によって、利用者の本人照合が記憶媒体中の情報によって実行されるため、簡便に本人照合を実行することが可能である。

【００３０】また、本発明は、前記利用者が前記記憶媒体を前記ネットワーク端末から取り外す取り外しステップと、前記記憶媒体が取り外された後、前記ネットワーク端末内の前記サービスアプリケーションが削除されるアプリケーション削除ステップと、を含むことを特徴とするネットワークサービス提供方法である。

【００３１】このような構成によって、記憶媒体が取り外された後、ネットワークサービスに使用していたソフトウェアを自動的に削除することが可能である。

【００３２】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【００３３】実施の形態１

図１は、本実施の形態１のネットワークサービスの提供が実施されるネットワークシステム１０の構成図である。

【００３４】この図に示すように、ネットワークシステム１０は、インターネット１２と、このインターネット１２に接続する認証／課金サーバ１４と、インターネット１２に接続するサービスサーバ群１６と、を備えている。

【００３５】インターネット１２には、ネットワークサービスの提供を受けるネットワーク端末１８が接続されている。利用者はこのネットワーク端末１８を用いてネットワークサービスの提供を受ける。

【００３６】本実施の形態において特徴的なことは、ネットワーク端末１８には、サービス鍵２０が接続されることである。このサービス鍵２０にはネットワークサービスを受けるための種々の情報やソフトウェアが格納されており、利用者はこのサービス鍵２０をネットワーク端末１８に取り付けるだけで、ネットワークサービスの提供を受けることができる。サービス鍵２０は所定の情報が格納された記憶媒体を主要な構成要素とする鍵である。格納されている情報等の詳細については後述する。

【００３７】その結果、上述した種々の設定をあらかじめネットワーク端末１８にしておく必要がなく、利用者は容易にネットワークサービスの提供を受けることができる。

【００３８】以下、本実施の形態１におけるネットワークサービスの提供の動作の流れを詳細に説明する。

【００３９】Ａ．初期ユーザ登録

まず、所定のサービスの提供を受けたい利用者は、自分が受けたいサービスに関する情報を、サービス鍵２０等に登録する。この動作を表すフローチャートが図２に示されている。

【００４０】この図のステップＳ２－１においては、利用者がサービス鍵２０をネットワーク端末１８に取り付ける。サービス鍵２０は情報を記憶できる記憶媒体であればどのようなものでもかまわない。フロッピー（登録商標）ディスクやＣＤ－Ｒ等の記憶媒体でもよいが、たとえばフラッシュメモリを内蔵したＵＳＢ（Universal Serial Bus）プラグ等が好ましい。以下の説明では、特に断らない限り、このＵＳＢプラグでサービス鍵２０を構成した例を説明する。ＵＳＢの規格による各種機器はネットワーク端末１２の電源を落とさなくても取り付け・取り外しが可能であるため、サービス鍵２０の取り付け・取り外しを迅速に行うことが可能である。また、ＣＤ－Ｒ等を駆動するドライブ装置も不要であるため、サービス鍵２０だけでなく、ネットワーク端末１８も小型に構成することができる。

【００４１】次に、ステップＳ２－２においては、ネットワーク端末１８が、ネットワーク端末１８にサービス鍵２０が取り付けられたこと（接続されたこと）を検知する。上述したようにＵＳＢ規格によって接続される機

器は、電源を落とさなくても接続・切り離しが可能であり、接続の度に自動的にその接続状態を検出する仕組みは従来からよく知られている。

【００４２】ステップＳ２－３においては、検知したサービス鍵２０からそのＵＳＢ機器のデバイスドライバが読み出される。そして、このデバイスドライバがネットワーク端末１８上で起動する。

【００４３】ステップＳ２－４においては、サービス鍵２０から初期化認証データ書き込みプログラムが読み出される。そして、この初期化認証データ書き込みプログラムがネットワーク端末１８上で起動する。このプログラムは、利用者が指定するデータを、サービス鍵２０内部に格納するためのプログラムである。このプログラムを利用することによって、利用者は自由に所定のデータをサービス鍵２０内部に格納することができる。

【００４４】ステップＳ２－５においては、利用者は、初期化認証データ書き込みプログラムの指示に従って、認証データを入力する。同様にして、利用者はクレジットカード番号も入力する。同様に、クレジットカードパスワードも入力する。

【００４５】なお、認証データとは、その利用者が本人であることを表すデータであり、種々のデータが利用される。指紋データやパスワードのデータ等が一般に認証データとして利用される。

【００４６】また、「認証データ」「クレジットカード番号」「クレジットカードパスワード」の３種のデータを本文では、「個人データ」と総称する。

【００４７】ステップＳ２－６においては、これら入力されたデータが、初期化認証データ書き込みプログラムによってサービス鍵２０内部に書き込まれる。同時に、新たに登録されたサービスがサービス鍵２０内部のデータベースに登録される。このようなデータベースをサービス鍵２０内部に設けることによって、その利用者にそのようなサービスが許可されているかを知ることができる。

【００４８】ステップＳ２－７においては、これら入力されたデータが、初期化認証データ書き込みプログラムによって認証／課金サーバ１４に通知される。

【００４９】ステップＳ２－８においては、認証・課金サーバ１４が、上記通知されてきた各種データを認証・課金サーバ１４内部に登録する。

【００５０】ステップＳ２－９においては、サービス鍵２０に設けられている確認ランプ２０ｃ（図６参照）が点灯する。この点灯は、初期化認証データ書き込みプログラムによって実行される。利用者は、この確認ランプ２０ｃの点灯によって、初期ユーザ登録が完了したことを知ることができる。また、この確認ランプ２０ｃの点灯は、初期ユーザ登録が完了し、サービス鍵２０をネットワーク端末１８から取り外してもよいことも意味する。

【００５１】Ｂ．システム運用動作

以下、実際に利用者がサービス鍵２０を用いてサービスの提供を受ける動作を図３のフローチャートに基づき説明する。

【００５２】まずステップＳ３－１においては、利用者がサービス鍵２０をネットワーク端末１８に取り付ける。

【００５３】次にステップＳ３－２においては、ネットワーク端末１８が、ネットワーク端末１８にサービス鍵２０が取り付けられたこと（接続されたこと）を検知する。この動作は上記ステップＳ２－２と同様である。

【００５４】ステップＳ３－３においては、検知したサービス鍵２０から、そのサービス鍵２０を構成するＵＳＢ機器のデバイスドライバが読み出される。そして、このデバイスドライバがネットワーク端末１８上で起動する。この動作は上記ステップＳ２－３と同様である。

【００５５】ステップＳ３－４においては、サービス鍵２０からサービス用データベースと、サービスアプリケーションとが読み出される。サービス用データベースは、ネットワーク端末１８内部に格納され、サービスアプリケーションは、ネットワーク端末１８上で起動される。サービスアプリケーションは、利用者に所定のネットワークサービスを提供するためにネットワーク端末１８上で動作するソフトウェアである。特に、このサービスアプリケーションは、その起動後、ネットワーク端末１８の画面上にアプリケーションアイコンを表示させる。このアプリケーションアイコンは、所定のネットワークサービスを開始させるアイコンであり、利用者がこのアイコンをクリックすると、対応するネットワークサービスの提供が開始される。

【００５６】さて、上記サービス用データベースと、上記サービスアプリケーションとは圧縮してサービス鍵２０内部に格納しておくことも好ましい。圧縮して格納する場合には、ネットワーク端末１８上に格納、又は、ネットワーク端末１８上で起動する前に、一旦解凍する必要がある。ここで、圧縮とは圧縮符号化を行うことを意味し、特に可逆圧縮を意味する。

【００５７】また、サービス用データベースとは、利用者が利用できるネットワークサービスが記述されているデータベースである。

【００５８】また、この際、サービスアプリケーションが利用するミドルウェアをサービス鍵２０から読み出して利用することも好ましい。ミドルウェアを用いれば、サービスアプリケーションと、他のソフトウェアとを連携させることが可能である。

【００５９】ステップＳ３－５においては、利用者が認証データをネットワーク端末１８に対して入力する。

【００６０】ステップＳ３－６においては、利用者が入力した認証データと、既にサービス鍵２０内部に格納されている認証データとが照合される。その結果、両者が

一致しない場合には、図４のステップＳ４－１に移行し、一致する場合には、図４のステップＳ４－２に処理が移行する。なお、ここでいう「一致」とは、認証データの種類によって意味が異なる。パスワードの場合は、この「一致」は「完全一致」を意味するが、指紋データの場合は「同一人による認証データと認められるほど両データが近似」していることをいう。

【００６１】ステップＳ４－１においては、一致しなかった旨が認証・課金サーバ１４に送信される。そして、認証・課金サーバ１４は、その内部に格納されている認証課金データを削除する。

【００６２】ステップＳ４－２においては、上記ステップＳ４－１に引き続き、ネットワーク端末１８がサービス鍵２０の内部に格納されている「個人データ」を消去する。そして、ネットワークサービスの提供が中止される。ネットワークサービスを受けたい場合には、利用者は再び上述した「初期ユーザ登録」を実行しなければならない。

【００６３】ステップＳ４－３においては、利用者が、ある所定のネットワークサービスを受けるために、そのネットワークサービスのアプリケーションアイコンをクリックする。

【００６４】ステップＳ４－４においては、上記アイコンのクリックに応じて、サービスアプリケーションが、サービスの開始を認証／課金サーバ１４に通知する。このサービスは、従来知られている種々のネットワークサービスである。たとえば、インターネット上の動画配信サービス（テレビジョン放送）や、音楽データの配信、種々のデータベースへの接続サービス等である。

【００６５】なお、通知の際には、アプリケーションＩＤと呼ばれる識別子を用いた通知を行うのが好ましい。このアプリケーションＩＤは、提供するサービスの識別子である。このアプリケーションＩＤについては、後に説明する。

【００６６】ステップＳ４－５においては、上記ステップＳ４－４における通知に応じて認証／課金サーバ１４が課金を開始する。さらに、認証／課金サーバ１４は、課金が開始されたことをサービスサーバ（群）１６に通知する。

【００６７】ステップＳ４－６においては、上記ステップＳ４－５における通知に応じて、サービスサーバ１６が所定のサービスを開始する。

【００６８】ステップＳ４－７においては、サービスアプリケーションがサービスサーバ１６にアクセスすることによって、サービスを利用者に提供する。

【００６９】次に、図５のステップＳ５－１においては、サービスを停止するために、利用者が上記サービスアイコンを閉じる。すると、ステップＳ５－２においてサービスアプリケーションは、サービスアイコンを閉じたことを、認証／課金サーバ１４に通知する。

【００７０】ステップＳ５－３においては、上記ステップＳ５－２における通知に応じて認証／課金サーバ１４が課金を停止する。また、認証／課金サーバ１４は課金を停止したことをサービスサーバ１６に通知する。

【００７１】ステップＳ５－４においては、上記ステップＳ５－３における通知に応じてサービスサーバ１６がサービスを停止する。

【００７２】そして、ステップＳ５－５においては、利用者がサービス鍵２０をネットワーク端末１８から取り外す。

【００７３】ステップＳ５－６においては、サービス鍵２０が取り外されたことに応じて、サービス鍵２０から展開したすべてのデータ（ソフトウェアを含む）がネットワーク端末１８から削除される。この削除は、誰が行ってもかまわないが、本実施の形態ではサービス鍵２０のデバイスドライバが削除を行っている。本実施の形態ではサービス鍵２０はフラッシュメモリを内蔵したＵＳＢプラグを利用しているため、上記デバイスドライバは、ＵＳＢのデバイスドライバである。

【００７４】以上述べたように、本実施の形態１によれば、サービス鍵２０をネットワーク端末１８に取り付けることによって、煩雑な設定をすることなくネットワーク端末１８がある場所であればどこでも、ネットワークサービスの提供を受けることができる。

【００７５】実施の形態２（サービス鍵の構成）

上記実施の形態１では、サービス鍵２０は、フラッシュメモリを内蔵したＵＳＢプラグを利用した。このようなサービス鍵２０の構成図が図６に示されている。

【００７６】この図に示すように、サービス鍵２０は、ＵＳＢプラグの本体２０ａ内にフラッシュメモリ２０ｂを内蔵している。このフラッシュメモリ２０ｂには、上述したように種々のデータ、ソフトウェアが格納されている。それらのデータ、ソフトウェアを列挙すれば以下の通りである。

【００７７】（１）デバイスドライバ：本実施の形態ではサービス鍵２０がＵＳＢプラグを利用しているため、このデバイスドライバはＵＳＢドライバである。サービス鍵２０として別の形態を採用する場合には、他の種類のデバイスドライバを採用する。

【００７８】（２）ミドルウェア：次のサービスアプリケーションを動作させるためのソフトウェアである。

【００７９】（３）サービスアプリケーション：ネットワークサービスを提供するソフトウェアである。このサービスアプリケーションは、基本的には、提供するサービスの個数だけ必要である。もちろん、１個のサービスアプリケーションで複数のサービスに対応させてもよい。

【００８０】（４）（個人）認証データ：指紋データやパスワード等である。このデータは、初期ユーザ登録を行う際に格納される。

【００８１】（５）認証／課金サーバ１４へのネットワーク設定データ：このデータは、認証／課金サーバ１４に認証を実行してもらい、課金を行うために必要な設定データであり、上述したクレジットカード番号等が含まれるデータである。このデータも、上記初期ユーザ登録においてサービス鍵２０内に書き込まれる。

【００８２】（６）認証／課金サーバ１４が認識可能なアプリケーションＩＤ：このＩＤは、利用者が複数のサービスを利用可能な場合に、どのサービスに対する認証／課金を行うべきかを識別するためのＩＤである。すなわちサービスの識別子である。

【００８３】（７）課金用のクレジットカード番号：このデータは課金用のクレジットカードの番号である。認証／課金サーバ１４は、このクレジットカード番号を利用して課金を行う。

【００８４】（８）データベース：このデータベースには、このサービス鍵２０の利用者に対して認められているサービスが登録されている。このデータベースは、上記初期ユーザ登録において更新される。特に、このようなデータベースを設けることによって、複数のサービスアプリケーションをあらかじめサービス鍵２０内部に格納しておくことが可能である。その利用者に許可されているサービスの情報がデータベースに登録されており、登録されているサービスのみに関しサービスアプリケーションが起動するように構成している。その結果、データベースに登録されていないサービス、すなわちその利用者に許可されていないサービスを誤ってその利用者に提供してしまうことがなくなる。

【００８５】これらのデータ、ソフトウェア群は、適宜、圧縮（圧縮符号化）を行ってサービス鍵２０のフラッシュメモリ２０ｂに格納しておくことが望ましい。また、ネットワークを介して外部に送られるデータ、たとえば認証／課金サーバ１４に送られる上記（４）～（７）のデータは、他人に流用されることを防止するために暗号化を施しておくことが望ましい。

【００８６】また、図６に示されるように、サービス鍵２０には、本発明の発光手段に相当する確認ランプ２０ｃが設けられている。この確認ランプ２０ｃは発光ダイオード等から構成され、その点灯状態は外部のネットワーク端末１８から制御される。確認ランプ２０ｃの動作については既に上で説明した。

【００８７】また、図６に示されるように、サービス鍵２０には、ＵＳＢプラグ部２０ｄが設けられている。このＵＳＢプラグ部２０ｄは、ネットワーク端末１８に設けられているＵＳＢインターフェースと勘合して電気的に接続するのである。

【００８８】本実施の形態１、２では、サービス鍵２０としてネットワークインターフェースであるＵＳＢインターフェースを備えた構成を採用したが、上記のような情報が格納されているＣＤ－Ｒ、フロッピーディスク等の単なる記憶媒体でももちろんかまわない。このような記憶媒体の場合には、ネットワーク端末１８はそれらの記憶媒体に対してデータの読み書きを実行できるドライブ装置（本発明における）「読み書き手段」）が備えられている必要がある。

【００８９】実施の形態３（ネットワーク端末の構成）

ネットワーク端末１８は、ネットワークに接続しうる種々の電子機器を利用することができる。典型的にはいわゆるパーソナルコンピュータをネットワーク端末１８として利用することができる。さらに、ネットワークに接続しているルータやサーバを本実施の形態におけるネットワーク端末１８として利用することも好ましい。

【００９０】これらのネットワーク端末１８は、サービス鍵２０を接続し、その内部のデータやソフトウェアの読み・書きが可能な手段を備えている必要がある。

【００９１】たとえば、上記図６で示したＵＳＢプラグ型のサービス鍵２０を利用するためには、ネットワーク端末１８はＵＳＢインターフェースを備えている必要がある。

【００９２】実施の形態４（複数の利用者によるサービス鍵の共有その他の利用形態）

また、サービス鍵２０は個人が自分のサービス鍵２０を携帯し、必要に応じて近くにあるネットワーク端末１８にそのサービス鍵２０を接続してネットワークサービスの提供を受けるのが典型的な利用形態であるが、１個のサービス鍵２０を複数の利用者が共有することも好ましい運用形態である。

【００９３】さらに、サービス鍵２０内部には複数のサービスアプリケーションを格納しておくことも好ましく、初期ユーザ設定を各サービス毎に行えば、１個のサービス鍵２０で複数のネットワークサービスの提供を受けることが可能である。

【００９４】その一方、各サービス毎に別個のサービス鍵２０を準備することも好ましい。１個のサービス鍵２０に常に１個のサービスを対応させればサービス鍵２０の管理が煩雑にならず、管理が容易になる。

【００９５】また、ｏｆｆｉｃｅ用途にも拡張することが可能である。

【００９６】実施の形態５（課金）

課金は認証課金サーバ１４が行うが、この課金は種々の課金体系を採用することができる。提供するサービスの回数によって課金してもよいし、また、サービスによって転送されたデータ量に基づき課金することも好ましい。さらに、サービスアイコンが開かれている間の時間によって課金を行うことも好ましい。

【００９７】以上述べたように本実施の形態１～３によれば、サービス鍵２０を個人が保持し、各種のネットワーク端末に取り付けることによって、利用者は特定のネットワークの設定を意識することなく、簡易にネットワーク上の種々のサービスを受けることができる。したが

って、サービス鍵２０さえ保持していれば、ネットワーク端末１８が設置されている任意の場所から所定のネットワークサービスを受けることが可能である。

【００９８】実施の形態６（その他）

なお、サービスサーバ１６は１個以上であれば何個でもかまわない。また、１個のサービスサーバ１６が複数種類のサービスを提供してもよい。また、各サービスが別個のサービスサーバからそれぞれ独立して提供されてもよい。

【００９９】認証／課金サーバ１４も１個以上であれば何個でもかまわない。各サービス毎に異なる認証／課金サーバ１４を利用してもよい。

【０１００】

【発明の効果】以上述べたように、本発明によれば、利用者は簡便にネットワークサービスを受けることが可能である。

【０１０１】また、本発明によるネットワーク端末（たとえば、ルータやサーバ）の位置する場所であればどこでも、利用者はネットワークサービスの提供を受けることが可能となる。

【０１０２】また、本発明のサービス鍵によれば、ネットワークサービスを受けるために必要な情報が格納されており、かつ、電子機器に接続しうるインターフェースも備えているため、このサービス鍵を各種電子機器に接続して、利用者がネットワークサービスの提供を受けることが可能となる。

【０１０３】また、本発明によれば、記憶媒体内のサービスアプリケーションが起動するので、利用者は簡便にネットワークサービスの提供を受けることができる。さらに、記憶媒体内の情報に基づいて本人認証を行うので、本人認証を簡便に実行可能である。そして、記憶媒体をネットワーク端末から取り外すと、ネットワーク端末内部のソフトウェアが削除される。

【図面の簡単な説明】

【図１】本発明の好適な実施の形態のネットワークシステムの構成図である。

【図２】実施の形態における初期ユーザ登録動作を表すフローチャートである。

【図３】実施の形態において、利用者がサービス鍵を用いてサービスの提供を受ける動作を表すフローチャートである。

【図４】実施の形態において、利用者がサービス鍵を用いてサービスの提供を受ける動作を表すフローチャートである。

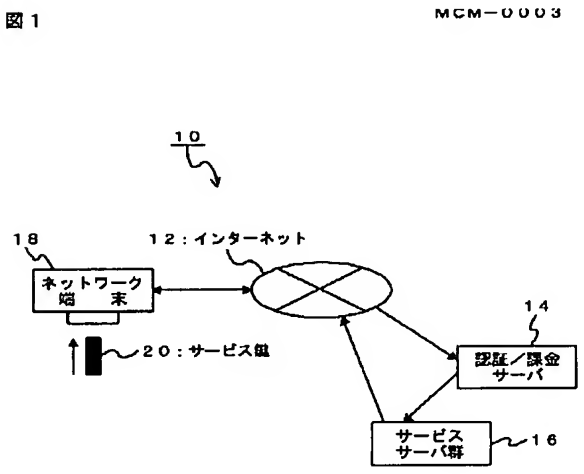
【図５】実施の形態において、利用者がサービス鍵を用いてサービスの提供を受ける動作を表すフローチャートである。

【図６】実施の形態におけるサービス鍵の構成図である。

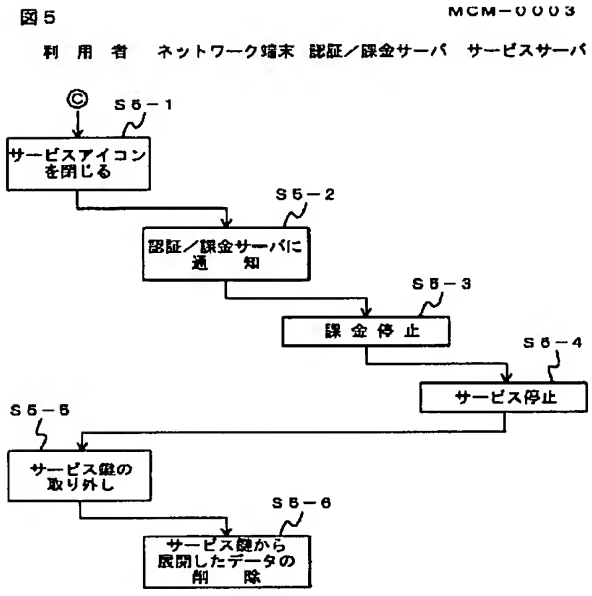
【符号の説明】

１０　ネットワークシステム
１２　インターネット
１４　認証／課金サーバ
１６　サービスサーバ群
１８　ネットワーク端末
２０　サービス鍵
２０ａ　本体
２０ｂ　フラッシュメモリ
２０ｃ　確認ランプ
２０ｄ　ＵＳＢプラグ部

【図１】



【図５】



【図２】

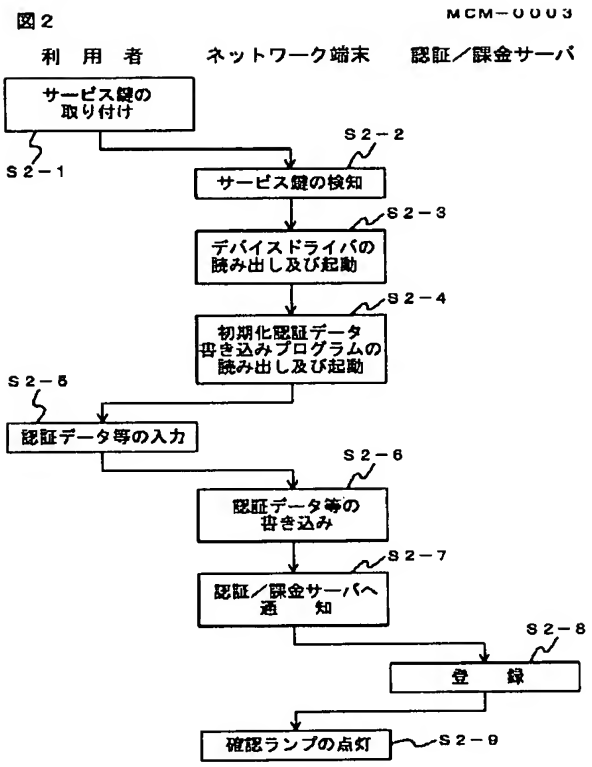


図２
MCM−0003
利　用　者
ネットワーク端末
認証／課金サーバ
サービス鍵の取り付け
S２−１
S２−２
サービス鍵の検知
S２−３
デバイスドライバの読み出し及び起動
S２−４
初期化認証データ書き込みプログラムの読み出し及び起動
S２−５
認証データ等の入力
S２−６
認証データ等の書き込み
S２−７
認証／課金サーバへ通　知
S２−８
登　録
確認ランプの点灯
S２−９

【図３】

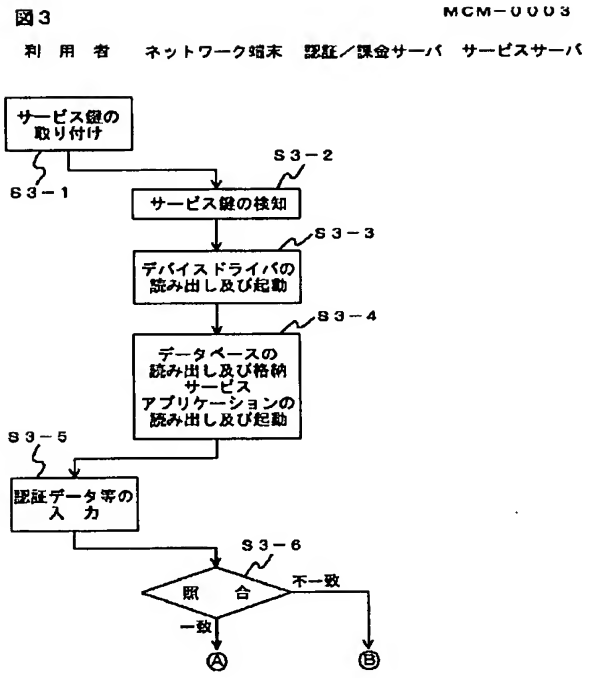


図３
MCM−0003
利　用　者
ネットワーク端末
認証／課金サーバ
サービスサーバ
サービス鍵の取り付け
S３−１
S３−２
サービス鍵の検知
S３−３
デバイスドライバの読み出し及び起動
S３−４
データベースの読み出し及び格納サービスアプリケーションの読み出し及び起動
S３−５
認証データ等の入　力
S３−６
照　合
不一致
一致
Ⓐ
Ⓑ

【図６】

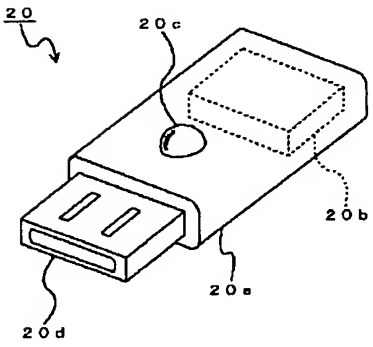


図６
MCM−0003
２０
２０ｃ
２０ｂ
２０ａ
２０ｄ

【図４】

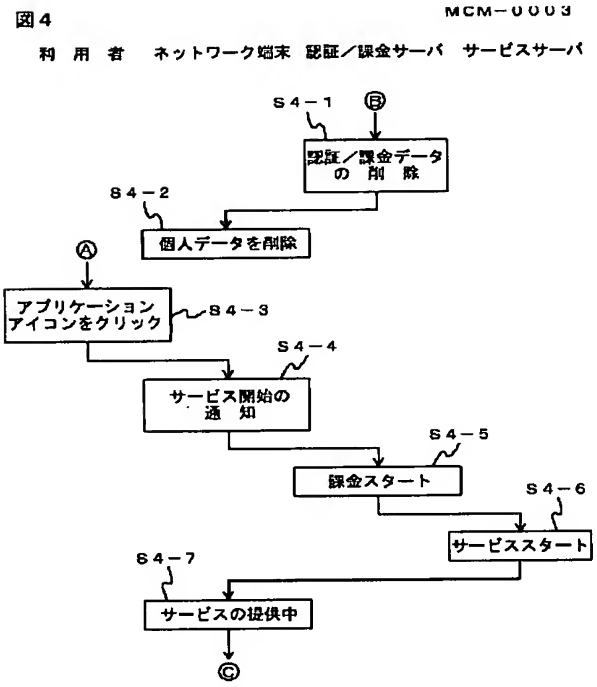


図４
MCM−0003
利　用　者
ネットワーク端末
認証／課金サーバ
サービスサーバ
S４−１
Ⓑ
認証／課金データの削除
S４−２
個人データを削除
Ⓐ
アプリケーションアイコンをクリック
S４−３
S４−４
サービス開始の通　知
S４−５
課金スタート
S４−６
サービススタート
S４−７
サービスの提供中
Ⓒ